(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 01 390 A 1**

(51) Int. Cl.[6]:
H 04 L 9/10
H 04 L 12/22
H 01 L 23/552
H 01 L 23/06
G 06 K 19/073

(21) Aktenzeichen: 196 01 390.9
(22) Anmeldetag: 16. 1. 96
(43) Offenlegungstag: 17. 7. 97

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Gruber, Martin, 92421 Schwandorf, DE

(56) Entgegenhaltungen:
US 52 33 563
US 51 59 629
US 50 53 992
DE-Z.: BETIRAC, Michael et al.: Mehr Sicherheit für Prozessorkarten. In: Funkschau, 1991, H. 20, S. 76-78;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Mikrochip mit einem diesen ganz oder teilweise umgebenden lichtundurchlässigen Ummantelungsabschnitt

(57) Es wird ein Mikrochip mit einem diesen ganz oder teilweise umgebenden lichtundurchlässigen Ummantelungsabschnitt beschrieben. Der beschriebene Mikrochip zeichnet sich dadurch aus, daß an einer Stelle, an welche nur unter bestimmungsfremder Entfernung und/oder Zerstörung des Ummantelungsabschnittes oder Teilen desselben Licht gelangen kann, ein lichtempfindliches Element vorgesehen ist.

196 01 390 A 1

Die vorliegende Erfindung betrifft einen Mikrochip mit einem diesen ganz oder teilweise umgebenden lichtundurchlässigen Ummantelung.

Derartige Mikrochips sind beispielsweise in Form von Mikrocomputern, Mikrocontrollern, Signalprozessoren, Speicherbausteinen und dergleichen bekannt.

Die Ummantelung erfüllt dabei je nach Mikrochip-Typ verschiedene Aufgaben. Während sie in den meisten Fällen in erster Linie zum Schutz vor mechanischen Beschädigungen dient, gibt es zunehmend auch Mikrochips, bei denen durch die Ummantelung alternativ oder zusätzlich eine optische und/oder elektrische Analyse des ummantelten Mikrochips ausgeschlossen werden soll.

Letztere Funktion der Ummantelung muß insbesondere bei solchen Mikrochips erfüllt sein, welche in Sicherheitsanwendungen (z. B. Chipkarten für Zugangsberechtigungen und dergleichen) eingesetzt werden. Die Ummantelung bzw. sicherheitsrelevante Bereiche des Mikrochips bedeckende Ummantelungsabschnitte (im folgenden der Einfachheit halber kurz als Ummantelung bezeichnet) solcher Mikrochips werden daher z. T. lichtundurchlässig ausgebildet. Darüber hinaus ist es jedoch erforderlich, zusätzlich dafür Sorge zu tragen, daß ein Mikrochip auch nach der Entfernung und/oder der Zerstörung der Ummantelung nicht analysiert werden kann.

Die zu diesem Zweck getroffenen Maßnahmen bestehen derzeit darin, daß die Ummantelung aus einem derartigen Material und/oder unter einer derartigen Verbindung mit dem Mikrochip hergestellt wird, daß ein den Mikrochip unversehrt lassendes vollständiges Entfernen und/oder Zerstören der Ummantelung ausgeschlossen ist oder aber zumindest sehr erschwert wird.

Derartige Vorkehrungen stellen zwar bereits einen relativ sicheren Schutz des Mikrochips dar, doch wird insbesondere aufgrund des enormen Sicherheitsrisikos, das eine Analysierbarkeit des Mikrochips mit sich bringen würde, weltweit nach weiteren Maßnahmen gesucht, durch welche eine Analyse von sicherheitsrelevanten Chips noch weiter erschwert werden kann.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, einen Mikrochip gemäß dem Oberbegriff des Patentanspruchs 1 derart weiterzubilden, daß eine Analyse des Mikrochips selbst nach gelungenem vollständigen Entfernen und/oder Zerstören der Ummantelung ausschließbar ist.

Diese Aufgabe wird erfindungsgemäß durch das im kennzeichnenden Teil des Patentanspruchs 1 beanspruchte Merkmal gelöst.

Demnach ist vorgesehen, daß an einer Stelle, an welche nur unter bestimmungsfremder Entfernung und/oder Zerstörung des Ummantelungsabschnittes oder Teilen desselben Licht gelangen kann, ein lichtempfindliches Element vorgesehen ist.

Diese Maßnahme hat den Effekt, daß auf das lichtempfindliche Element beim bestimmungsgemäßen Umgang mit dem Mikrochip kein Licht fällt, wohingegen beim bestimmungsfremden Umgang mit dem Mikrochip, d. h. bei Freilegen desselben durch Entfernen und/oder Zerstören der Ummantelung oder spätestens beim Versuch einer unter Beleuchtung durchzuführenden optischen Analyse oder einem ebenfalls unter Beleuchtung durchzuführenden Anschließen von Signalleitungen zum Auslesen von Speicherinhalten oder dergleichen zwangsläufig Licht auf das lichtempfindliche Element liche Element durch das lichtempfindliche Element ist unter diesen Umständen ein sicheres Anzeichen dafür, daß gerade ein Versuch unternommen wird, den Mikrochip zu analysieren.

Wird das Erfassen eines Lichteinfalls durch das lichtempfindliche Element daher beispielsweise dahingehend ausgewertet, daß als Reaktion darauf beispielsweise ein Löschen von Speicherinhalten und/oder ein Zerstören des Mikrochips oder dergleichen veranlaßt wird, ist eine Analyse selbst nach einem gelungenen vollständigen Entfernen und/oder Zerstören der Ummantelung des Mikrochips zuverlässig ausschließbar.

Vorteilhafte Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher erläutert.

Ausgangspunkt ist ein vor einer unbefugten Fremdanalyse zu schützender, beispielsweise (aber nicht ausschließlich) in einer Chipkarte enthaltener Mikrochip. Der Mikrochip kann ein beliebiges elektronisches Element sein; in der Regel wird es sich hierbei jedoch um eine integrierte Schaltung wie einen Mikroprozessor, Signalprozessor, Mikrocontroller, Speicherbaustein oder dergleichen handeln.

Der Mikrochip ist ganz oder teilweise von einem lichtundurchlässigen Ummantelungsabschnitt (im folgenden der Einfachheit halber kurz als Ummantelung bezeichnet) umgeben, um ihn mechanisch zu schützen und um eine optische Analyse von dessen Aufbau und Strukturen zu verhindern.

Die lichtundurchlässige Ummantelung bedeckt zumindest die sicherheitsrelevanten Bereich des Mikrochips.

Sofern auch eine elektrische Analyse des Mikrochips ausgeschlossen sein soll, sind auch die elektrischen Anschlußstellen des Mikrochips und die mit diesen verbundenen Signalleitungen, gegebenenfalls auch eine äußere Beschaltung des zu schützenden Mikrochips von der Ummantelung umgeben.

Die Ummantelung kann durch ein Gehäuse, ein gehäuseartiges Gebilde (beispielsweise Vergußmassen bzw. sogenannte Globe-Top-Abdeckungen bei in Chipkarten enthaltenen Mikrochips und dergleichen) oder ein Teil derselben gebildet werden; alternativ oder ergänzend kann sie auch durch ein über dem zu schützenden Mikrochip angeordnetes weiteres elektrisches, elektromechanisches oder mechanisches Bauelement, beispielsweise durch einen auf den zu schützenden Mikrochip direkt oder indirekt (d. h. unter Einfügung einer Isolationsschicht oder dergleichen) aufgesetzten zweiten Mikrochip, oder ein Teil desselben gebildet werden.

Erfindungsgemäß sind nun innerhalb des Mikrochip-Ummantelungsgebildes ein oder mehrere lichtempfindliche Elemente vorgesehen.

Die lichtempfindlichen Elemente können dabei in die Ummantelung integriert sein und/oder an der Oberfläche und/oder im Inneren des Mikrochips vorgesehen sein. Sie sind vorzugsweise über oder in unmittelbarer Nähe von denjenigen Stellen des Mikrochips angeordnet, dessen ungehinderte Freilegung für eine Analyse des Mikrochips förderlich sein könnte.

Bei bestimmungsgemäßem Umgang mit dem wie beschrieben ummantelten Mikrochip fällt auf das lichtempfindliche Element aufgrund der Lichtundurchlässigkeit der darüber liegenden Ummantelung nie Licht. Bei bestimmungsfremdem Umgang mit dem Mikrochip,

d. h. bei Freilegen desselben unter Entfernen und/oder Zerstören der Ummantelung oder spätestens beim Versuch einer unter Beleuchtung durchzuführenden optischen Analyse oder einem ebenfalls unter Beleuchtung durchzuführenden Anschließen von Signalleitungen zum Auslesen von Speicherinhalten oder dergleichen trifft hingegen zwangsläufig Licht auf das lichtempfindliche Element.

Dies löst in Abhängigkeit von der Art des lichtempfindlichen Elements unterschiedliche Vorgänge im lichtempfindlichen Element aus.

Ist das lichtempfindliche Element ein Speicherelement, dessen Inhalt beim Einfall von Licht veränderbar ist, kann dieser Speicherinhalt durch eine hierzu vorgesehene Steuereinrichtung (Sicherheitslogik) ausgewertet werden. Das Auslesen des Speicherelements und die Auswertung des Inhalts kann dabei zu beliebigen Anlässen (beispielsweise immer bei Anlegen einer Betriebsspannung) und/oder Zeitpunkten erfolgen. Wird dabei festgestellt, daß ein Lichteinfall auf das lichtempfindliche Element stattgefunden hat, also ein Versuch unternommen wird, den Mikrochip zu analysieren, wird dies zum Anlaß genommen, eine vom Typ des lichtempfindlichen Elements unabhängige, später noch genauer beschriebene Reaktion zu veranlassen.

Ist das lichtempfindliche Element ein fotoelektrisches Wandlerelement, das bei Lichteinfall eine Spannung erzeugt, kann diese Spannung dazu verwendet werden, eine vom Typ des lichtempfindlichen Elements unabhängige, später noch genauer beschriebene Reaktion zu veranlassen bzw. durchzuführen.

Ist das lichtempfindliche Element ein bei Lichteinfall seine elektrischen Eigenschaften veränderndes Element, können die veränderten elektrischen Eigenschaften zur Realisierung einer Schaltfunktion verwendet werden, mittels welcher eine vom Typ des lichtempfindlichen Elements unabhängige, später noch genauer beschriebene Reaktion veranlaßbar bzw. durchführbar ist.

Die Reaktion auf das Erfassen eines Lichteinfalls bzw. auf einen Lichteinfall besteht allgemein gesprochen darin, daß Maßnahmen getroffen werden, die eine Analyse des zu schützenden Mikroprozessors unmöglich machen. Die Reaktion kann beispielsweise darin bestehen, daß gespeicherte Informationen ganz oder teilweise gelöscht und/oder der Mikrochip oder einzelner Funktionen desselben zerstört werden (beispielsweise durch Zünden sogenannter Fußes). Darüber hinaus können auf das Erfassen eines Lichteinfalls hin bzw. auf einen Lichteinfall hin selbstverständlich auch beliebige andere Reaktionen ausgelöst werden, die die Analyse des zu schützenden Chips erschweren oder ausschließen.

Um zu verhindern, daß ein Lichteinfall auf das lichtempfindliche Element schon bei der Herstellung des Mikrochips die beschriebene Reaktion zeigt, ist gegebenenfalls ein Aktivierungsprozeß vorzusehen, durch welchen die ursprünglich noch nicht aktivierten Reaktionen aktivierbar sind, beispielsweise indem eine Sicherheitslogik irreversibel von einem Aus-Zustand in einen Bereitschaftszustand versetzt wird.

Die spektrale Empfindlichkeit des lichtempfindlichen Elements ist vorzugsweise so ausgelegt, daß nicht nur der Einfall von sichtbarem Licht, sondern auch der Einfall anderer Strahlungsarten, die zur Sichtbarmachung von Mikrochip-Strukturen verwendbar sind, durch das lichtempfindliche Element erfaßbar sind. Sofern das gesamte Strahlungsspektrum nicht durch ein einzelnes lichtempfindliches Element abgedeckt werden kann, [illegible] mehrere lichtempfindliche Elemente vorzusehen, die sich diesbezüglich ergänzen.

Die über einem lichtempfindlichen Element vorgesehene Chip-Ummantelung ist vorzugsweise so ausgebildet, daß sie für sämtliche Strahlungs-Wellenlängen, die durch das lichtempfindliche Element erfaßbar ist, undurchlässig ist; sofern bestimmte Strahlungswellenlängen in der Umgebung des zu schützenden Chips üblicherweise nicht vorkommen, kann es sich als vorteilhaft erweisen, die Ummantelung hierfür durchlässig zu gestalten.

Patentansprüche

1. Mikrochip mit einem diesen ganz oder teilweise umgebenden lichtundurchlässigen Ummantelungsabschnitt, **dadurch gekennzeichnet**, daß an einer Stelle, an welche nur unter bestimmungsfremder Entfernung und/oder Zerstörung des Ummantelungsabschnittes oder Teilen desselben Licht gelangen kann, ein lichtempfindliches Element vorgesehen ist.
2. Mikrochip nach Anspruch 1, dadurch gekennzeichnet, daß der Mikrochip Bestandteil einer Chipkarte ist.
3. Mikrochip nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Ummantelungsabschnitt durch ein gehäuseartiges Gebilde oder ein Teil desselben gebildet wird.
4. Mikrochip nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Ummantelungsabschnitt durch ein über dem Mikrochip angeordnetes weiteres Bauelement oder ein Teil desselben gebildet wird.
5. Mikrochip nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element und/oder eine gegebenenfalls vorgesehene Sicherheitslogik beim Erfassen eines Lichteinfalls auf das lichtempfindliche Element sofort oder später ein zumindest teilweises Löschen von gespeicherter Information und/oder ein Zerstören des Mikrochips oder Teilen desselben veranlassen.
6. Mikrochip nach Anspruch 5, dadurch gekennzeichnet, daß das lichtempfindliche Element und/oder die gegebenenfalls vorgesehene Sicherheitslogik derart ausgebildet sind, daß Art und Umfang von auf das Erfassen eines Lichteinfalls hin ausgeführte oder veranlaßte Reaktionen von einer vorherigen Aktivierung derselben abhängig machbar sind.
7. Mikrochip nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element ein auf einen Lichteinfall ansprechendes Speicherelement ist.
8. Mikrochip nach Anspruch 7, dadurch gekennzeichnet, daß eine Sicherheitslogik vorgesehen ist, welche die im Speicherelement gespeicherte Information zu gegebenen Anlässen und/oder zu gegebenen Zeitpunkten ausliest, auswertet und entsprechend darauf reagiert.
9. Mikrochip nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element ein fotoelektrisches Wandlerelement ist, welches bei Lichteinfall eine Spannung erzeugt.
10. Mikrochip nach Anspruch 9, dadurch gekennzeichnet, daß die erzeugte Spannung zum zumin-

oder Teilen desselben verwendet wird.

11. Mikrochip nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element ein bei Lichteinfall seine elektrischen Eigenschaften veränderndes Element ist.

12. Mikrochip nach Anspruch 11, dadurch gekennzeichnet, daß die veränderten elektrischen Eigenschaften zur Realisierung einer Schaltfunktion verwendet werden, mittels welcher eine ein zumindest teilweises Löschen von gespeicherter Information und/oder ein Zerstören des Mikrochips oder Teilen desselben veranlassende Spannung durchschaltbar ist.